# AUTOMATED VEHICLES

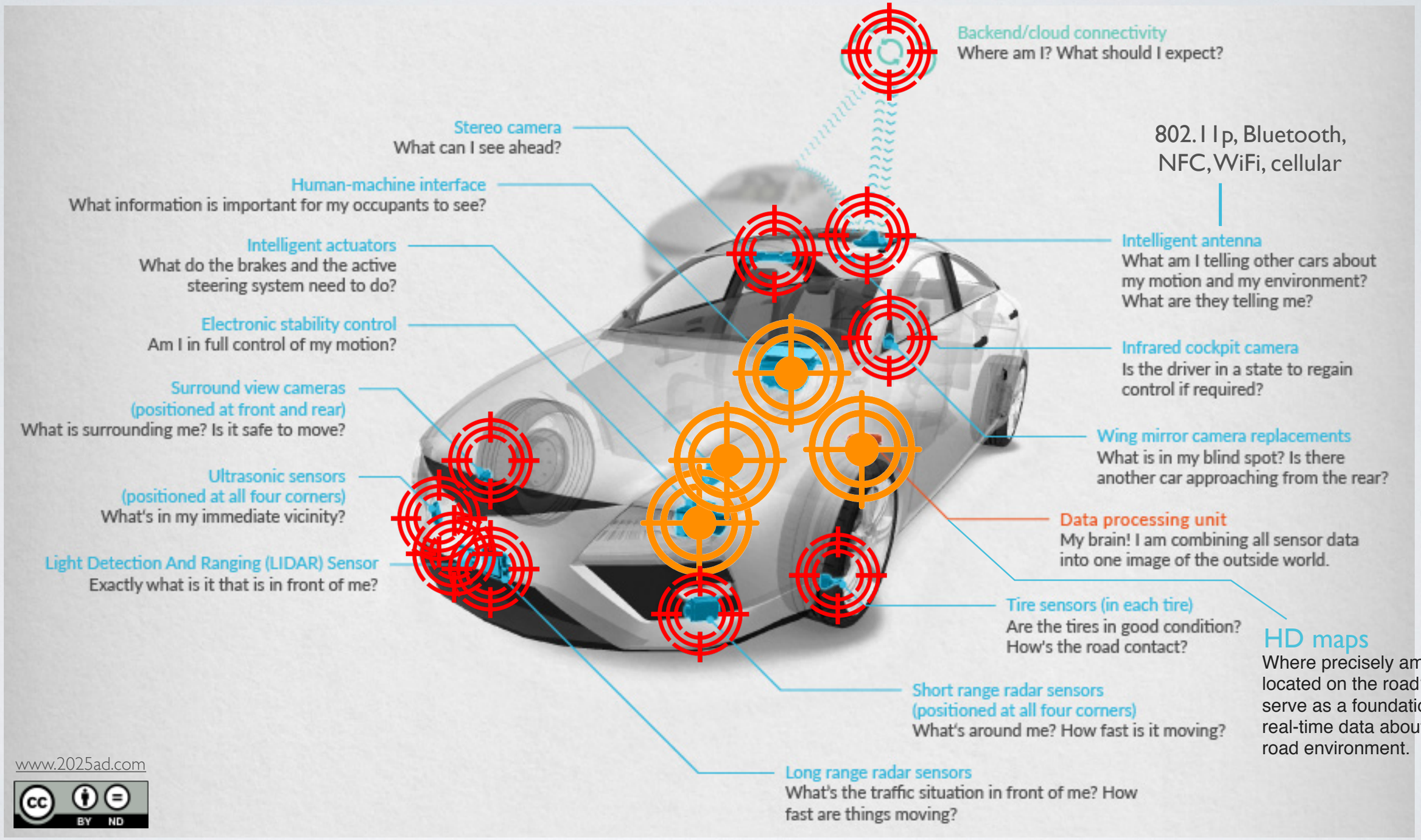
# SECURITY

Jonathan Petit

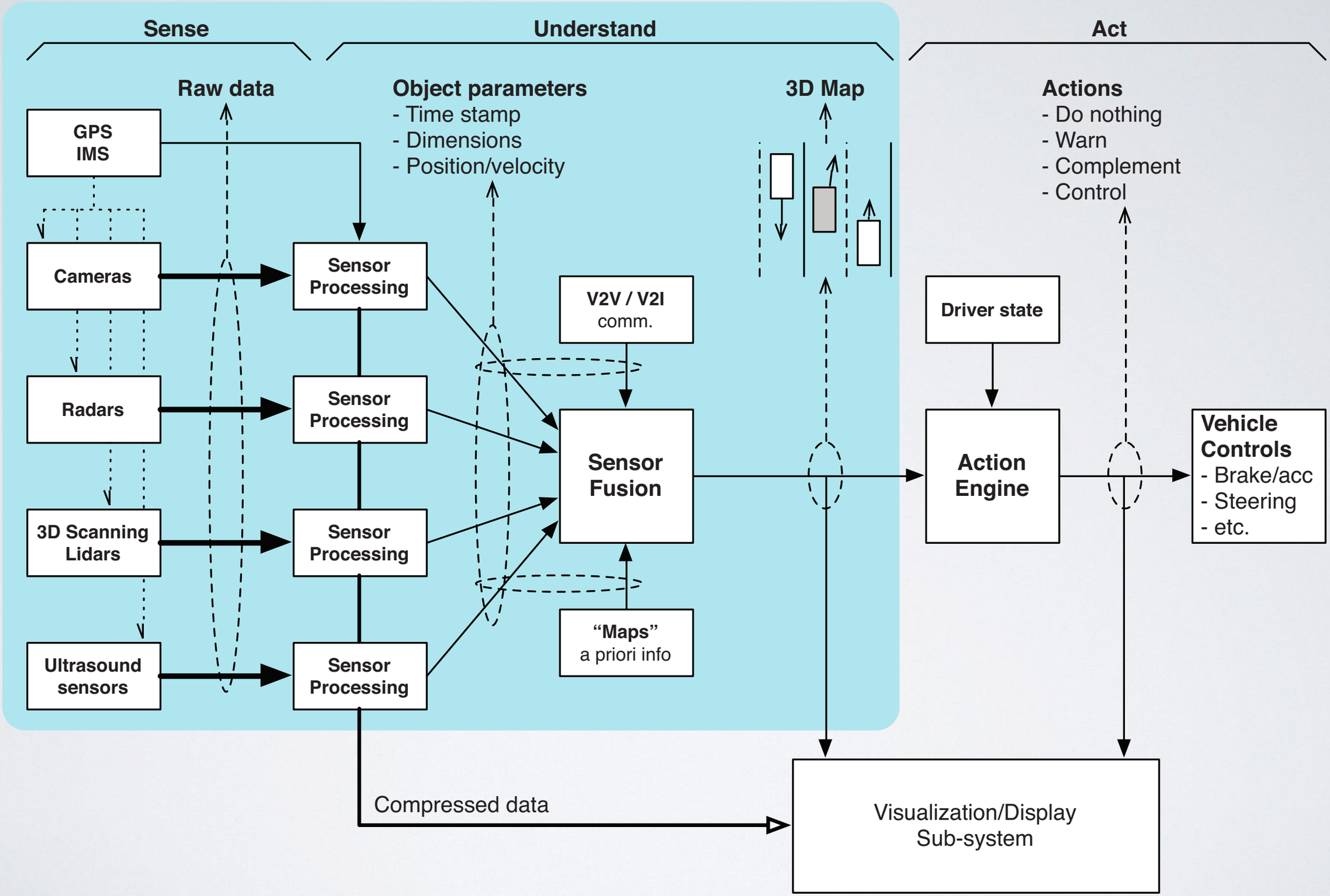
jpetit@securityinnovation.com

SECURITY INNOVATION
EMBEDDED

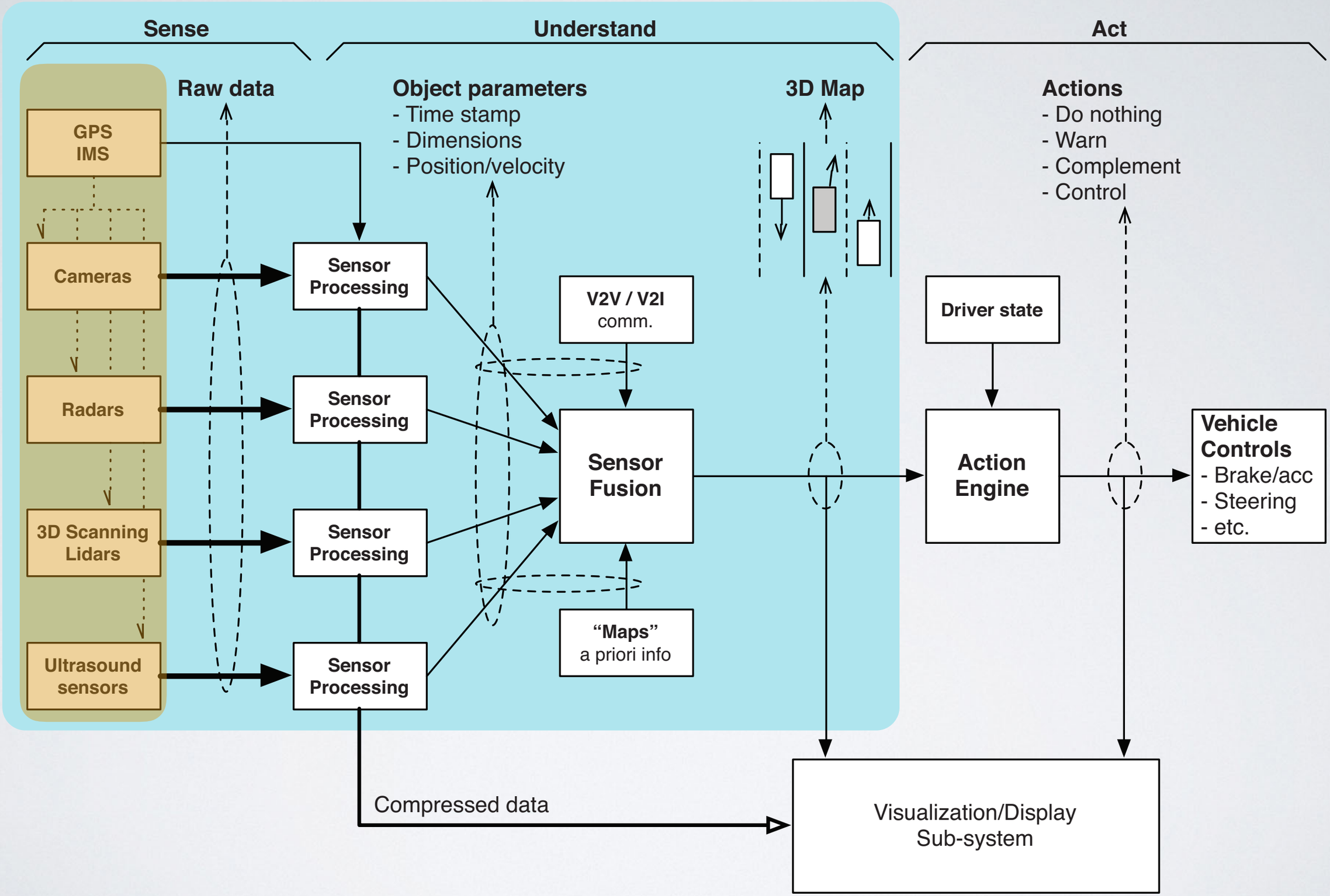
# AUTOMATED/CONNECTED VEHICLE




www.2025ad.com



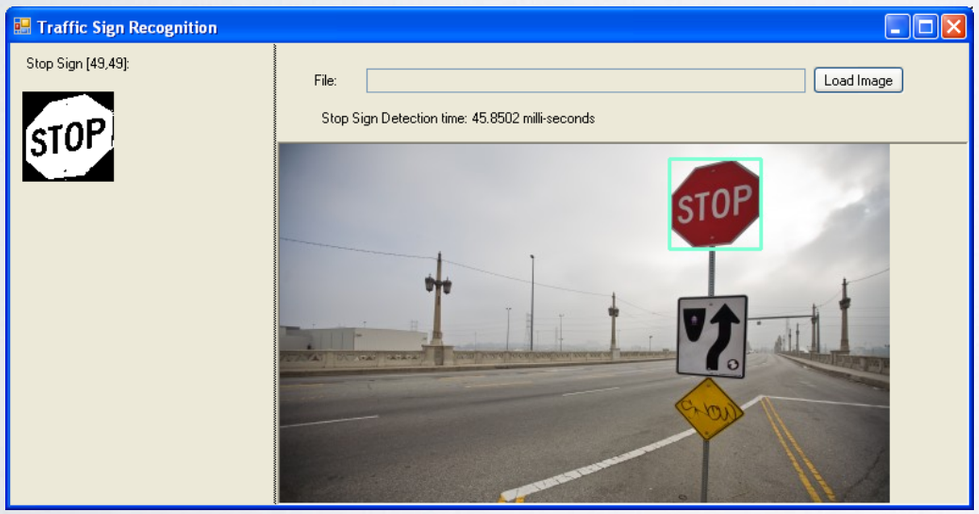

credit: F. Mujica. Scalable electronics driving autonomous vehicle technologies. Technical report, Autonomous Vehicles R&D, Kilby Labs, Texas Instruments, 2014.



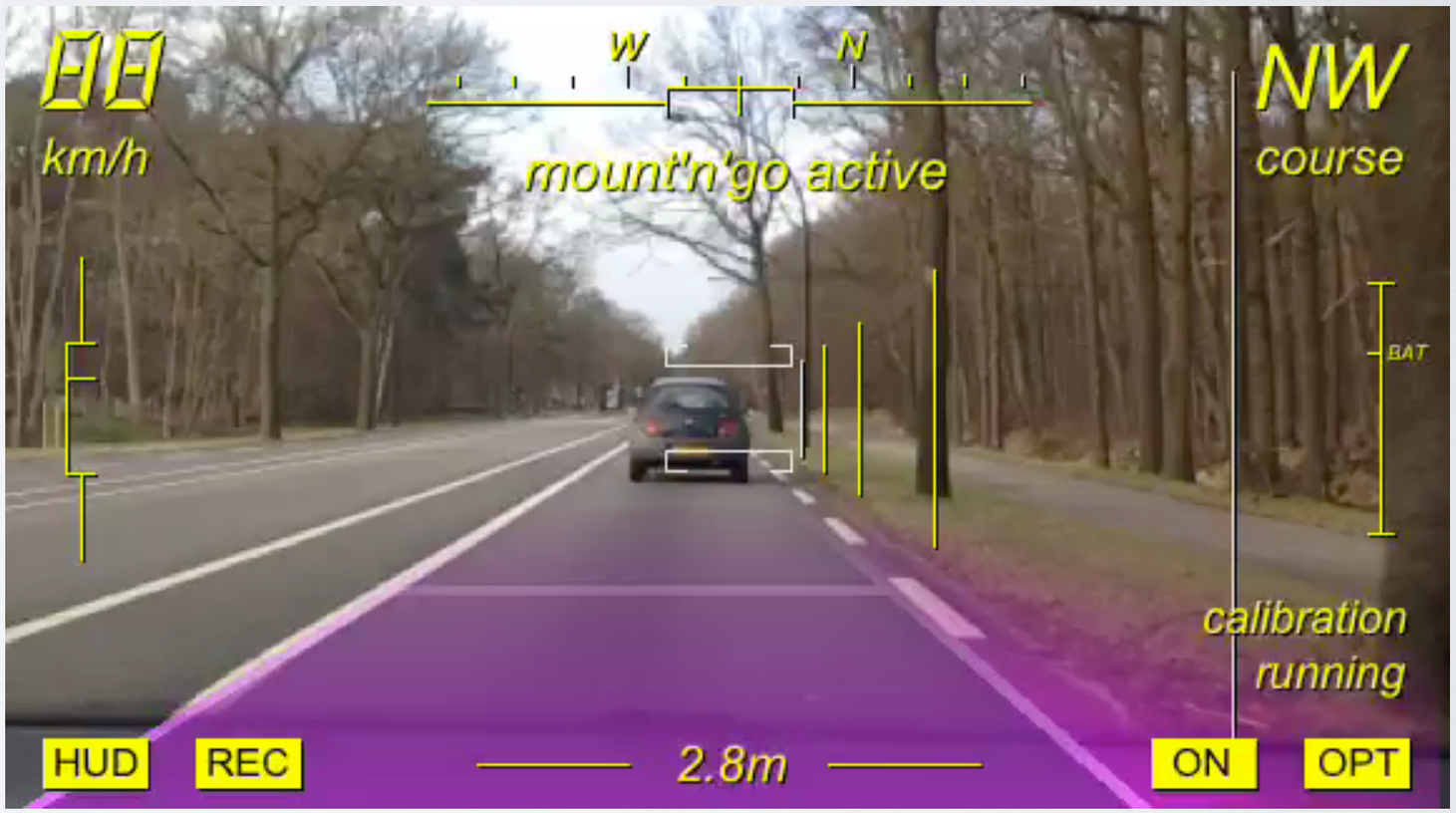

credit: F. Mujica. Scalable electronics driving autonomous vehicle technologies. Technical report, Autonomous Vehicles R&D, Kilby Labs, Texas Instruments, 2014.

# CAMERA

For now, the only sensor capable of reading traffic sign

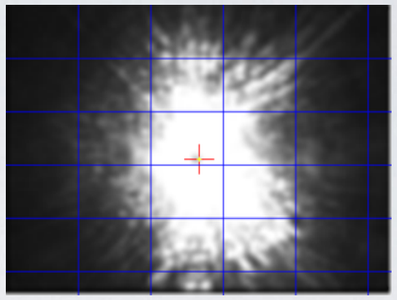


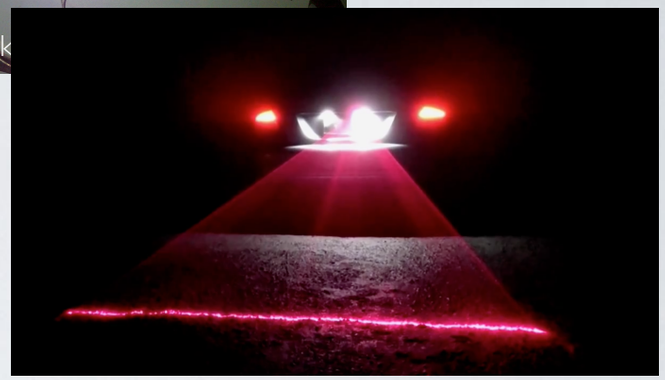

http://www.emgu.com/wiki/images/StopSignDetectionExample1.png




http://www.carstuff.com.tw/images/stories/LEE/20130427/130427_mobileye_1.jpg

- Blinding (partial, full)

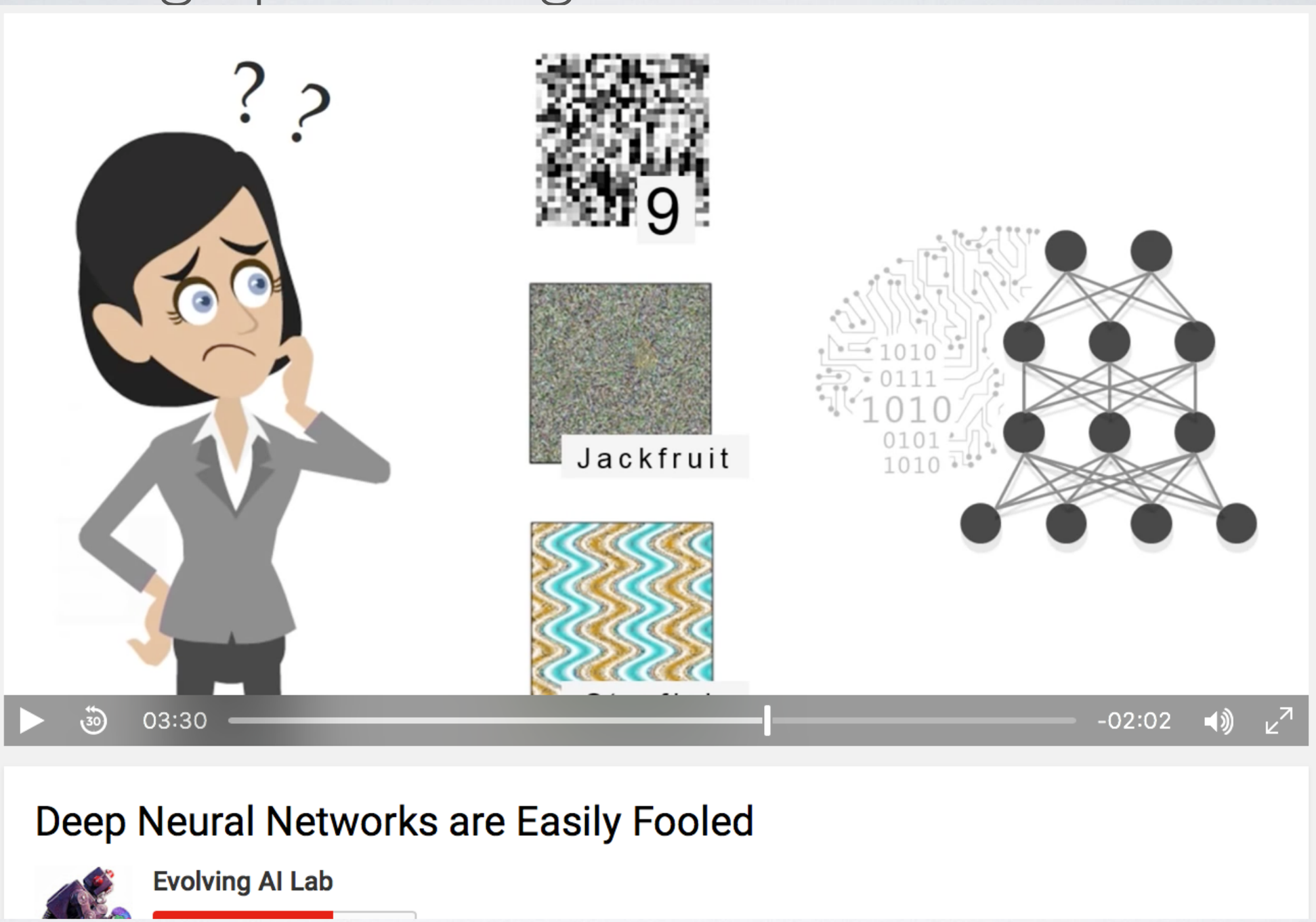


- Dazzle

- Confusion / modification


- Fool image processing




Nguyen, Anh, Jason Yosinski, and Jeff Clune. "Deep neural networks are easily fooled: High confidence predictions for unrecognizable images." *Computer Vision and Pattern Recognition (CVPR), 2015 IEEE Conference on*. IEEE, 2015.

# EXPERIMENT: FOOL CLASSIFIER

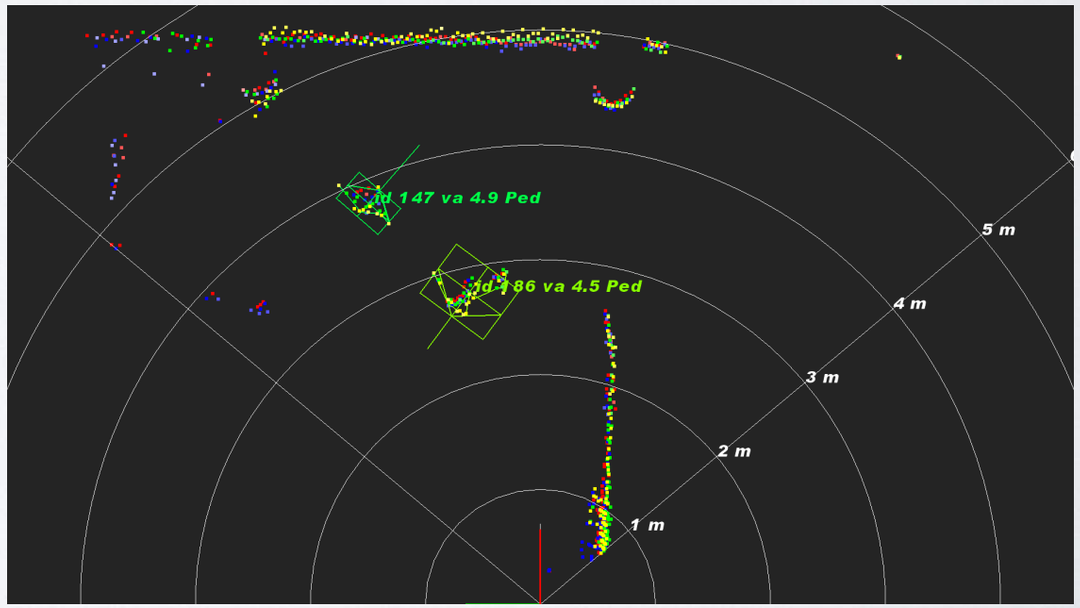
- Goal: **Build security test suites for vision-based system** and understand what an attacker can do.
  - Install camera on the roadside, and drive by while showing random noise pictures and check if classified.
  - Evaluate size of fake picture, distance to target
  - Identify the type of classifier used: linear, quadratic, cubic, RBF, nonlinear (neural, with breadth and *depth*) → different robustness[1]
  - Challenges: high-dimensional space, 3D image and video

[1] Fawzi, A., Fawzi, O., & Frossard, P. (2015). Analysis of classifiers' robustness to adversarial perturbations. *arXiv preprint arXiv:1502.02590*.

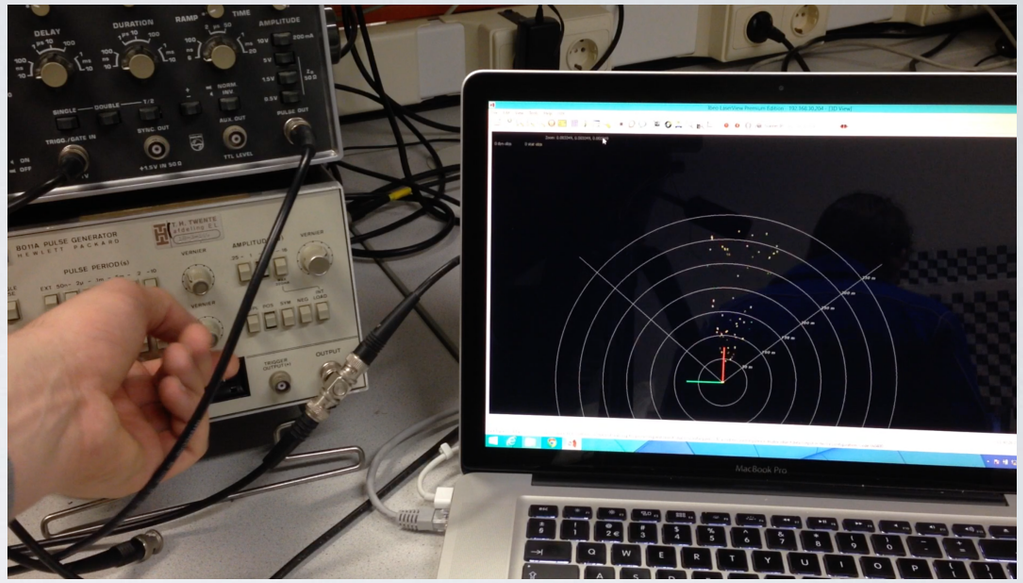
# LIDAR



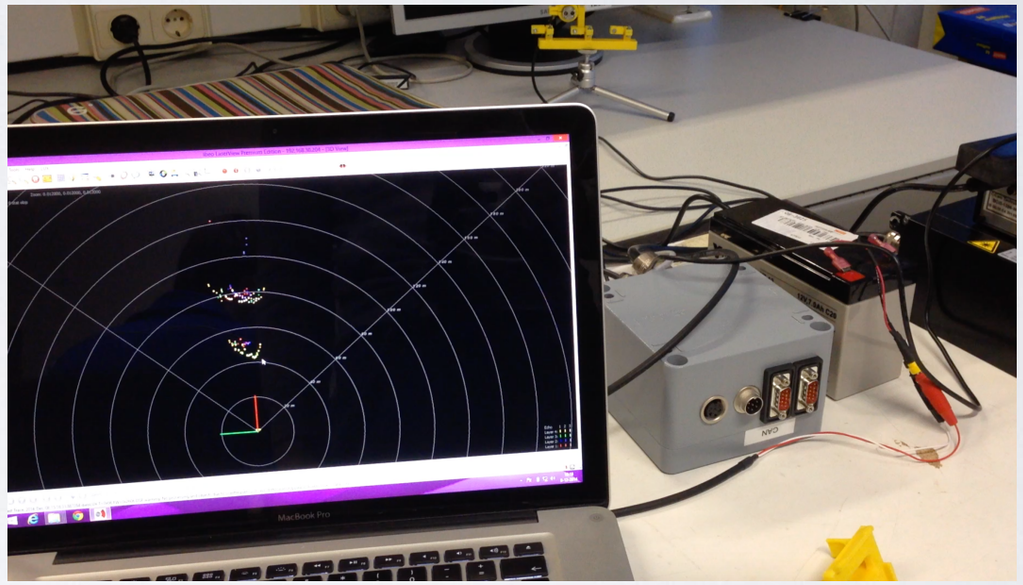
quanergy.com



- Jamming




- Spoofing



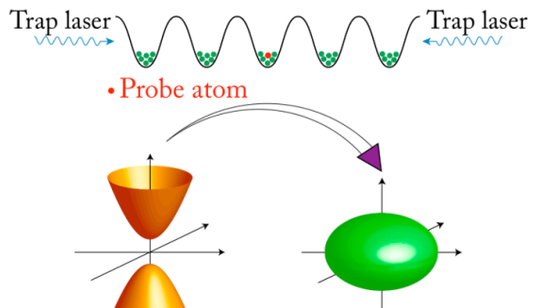

- Undetected objects

## Scientists Take a Major Leap Toward a 'Perfect' Quantum Metamaterial

Berkeley Lab, UC Berkeley researchers lead study that uses trapped atoms in an artificial crystal of light

News Release Glenn Roberts Jr. 510-486-5582 • **MAY 11, 2016**

Scientists have devised a way to build a "quantum metamaterial"—an engineered material with exotic properties not found in nature—using ultracold atoms trapped in an artificial crystal composed of light. The theoretical work represents a step toward manipulating atoms to transmit information, perform

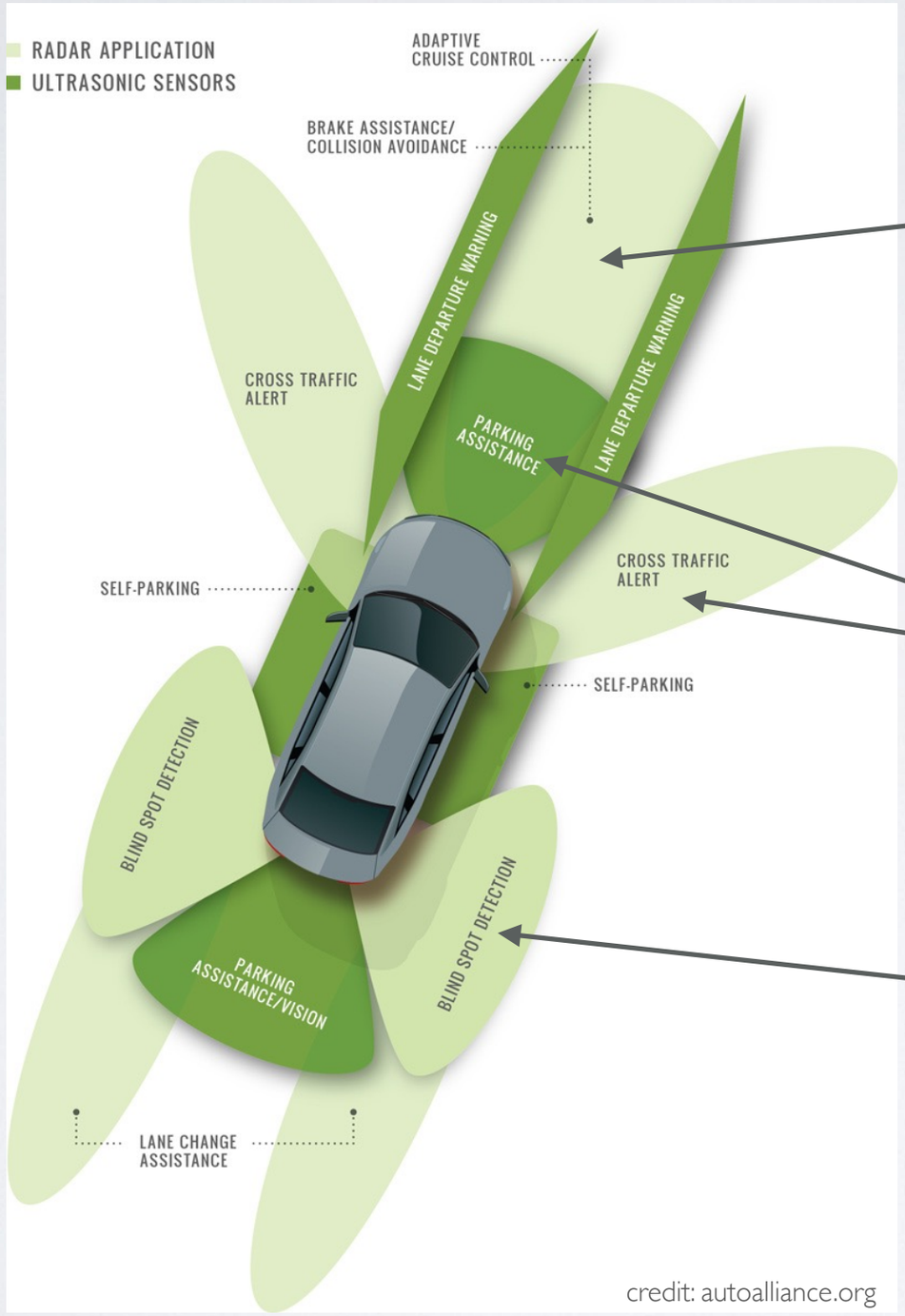


# EXPERIMENT: SPOOFING

- Goal: **Insert fake object while in motion**
  - follow-up of our BlackHat Europe paper
  - check effect of number of layers, information received per probes (reflectivity, power, etc.), distance and position of attacker

# RADAR

- Bi-static
- Mono-static
- Pulsed
- Continuous Wave
- Frequency-Modulated Continuous-Wave




credit: autoalliance.org

range: 200 meters
frequency: 76-77 GHz

range: 30 meters
frequency: 24 / 68 / 77-81 GHz

range: 20 meters
frequency: 24 / 76-77 GHz

SECURITY INNOVATION EMBEDDED

# EXPERIMENT: SPOOFING

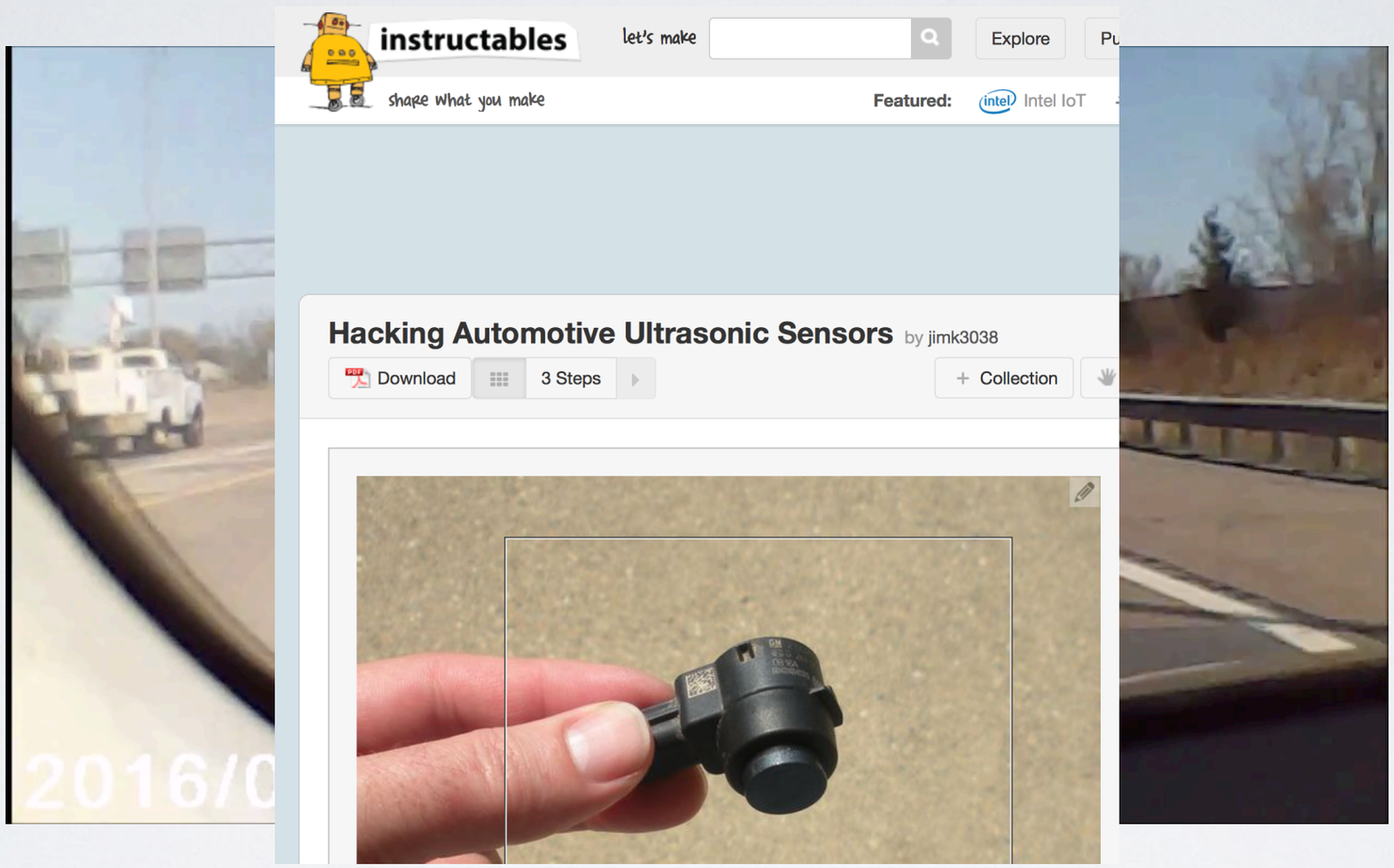
- **Goal: Fool long-range radar to remotely affect adaptive cruise control**

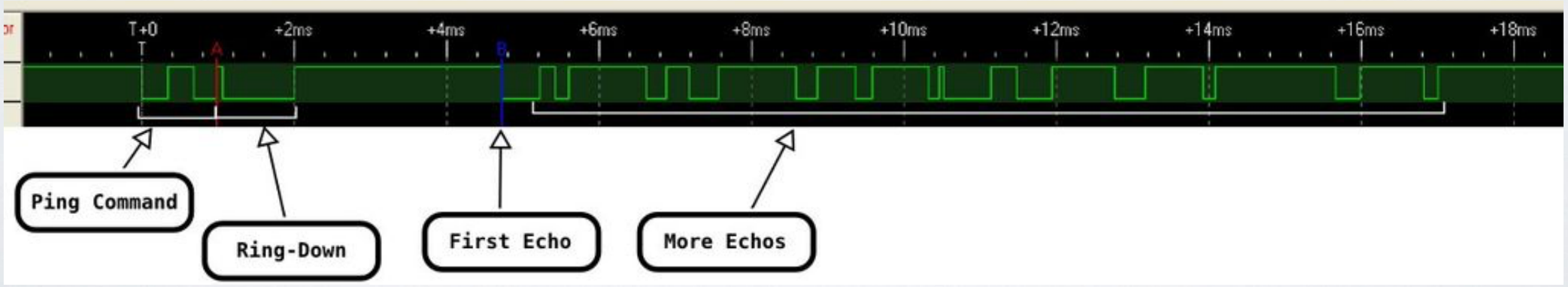
    1. Assess which frequency is in use
    2. Assess range of sensors and type of antenna to use (sensitivity, angular resolution, power pattern, EIRP)
    3. Build receiver/transmitter for the frequency
    4. Send fake echo to the sensor

- Note: see "deception jamming", Shi, Xiao-ran, et al. "Deception jamming method based on micro-Doppler effect for vehicle target." *IET Radar, Sonar & Navigation* (2016).

# ULTRASONIC SENSOR

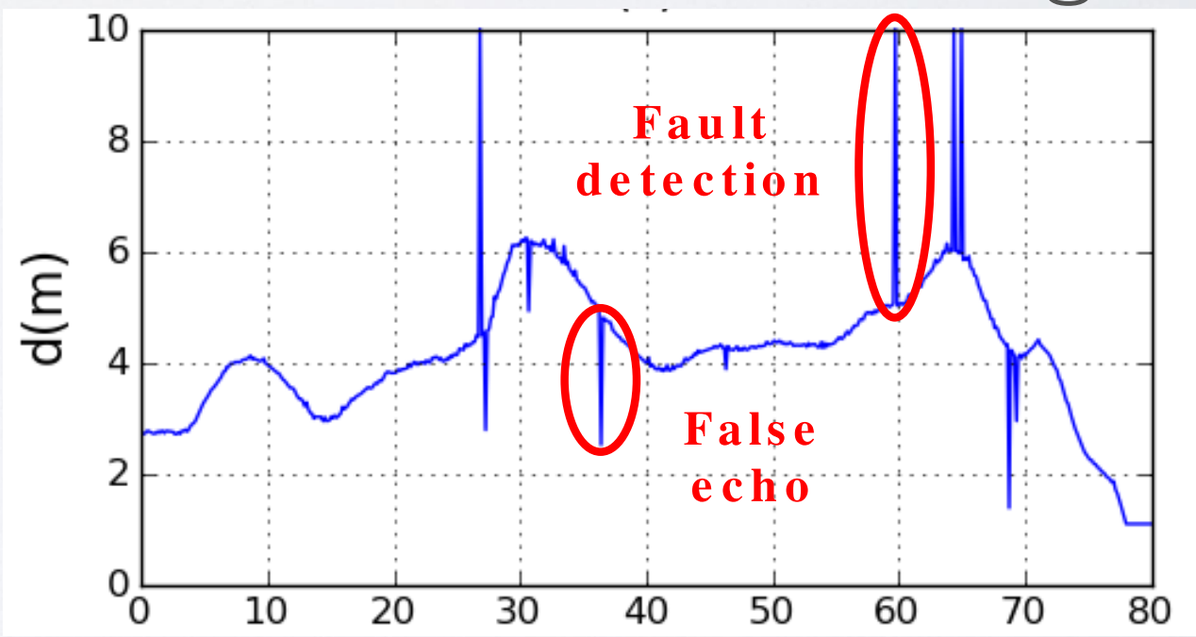
# ULTRASONIC SENSOR



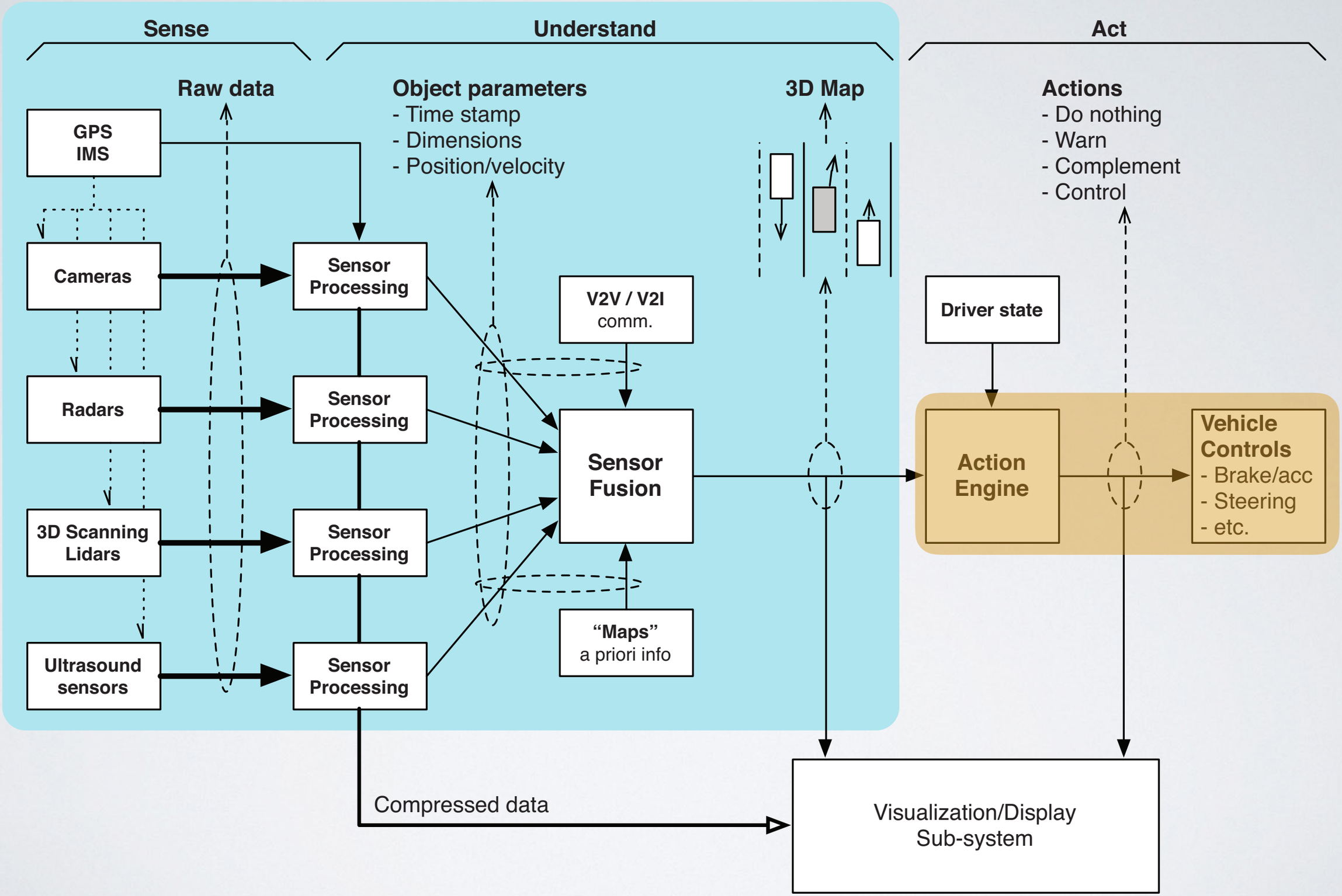



# EXPERIMENT

- **Goal: Force (semi) automated vehicle to stay on its lane or to take evasive action**
- Spoof fake echo
- To assess: maximum distance between target and attacker




Alonso, Luciano, et al. "Ultrasonic sensors in urban traffic driving-aid systems." *Sensors* 11.1 (2011): 661-673.




credit: F. Mujica. Scalable electronics driving autonomous vehicle technologies. Technical report, Autonomous Vehicles R&D, Kilby Labs, Texas Instruments, 2014.

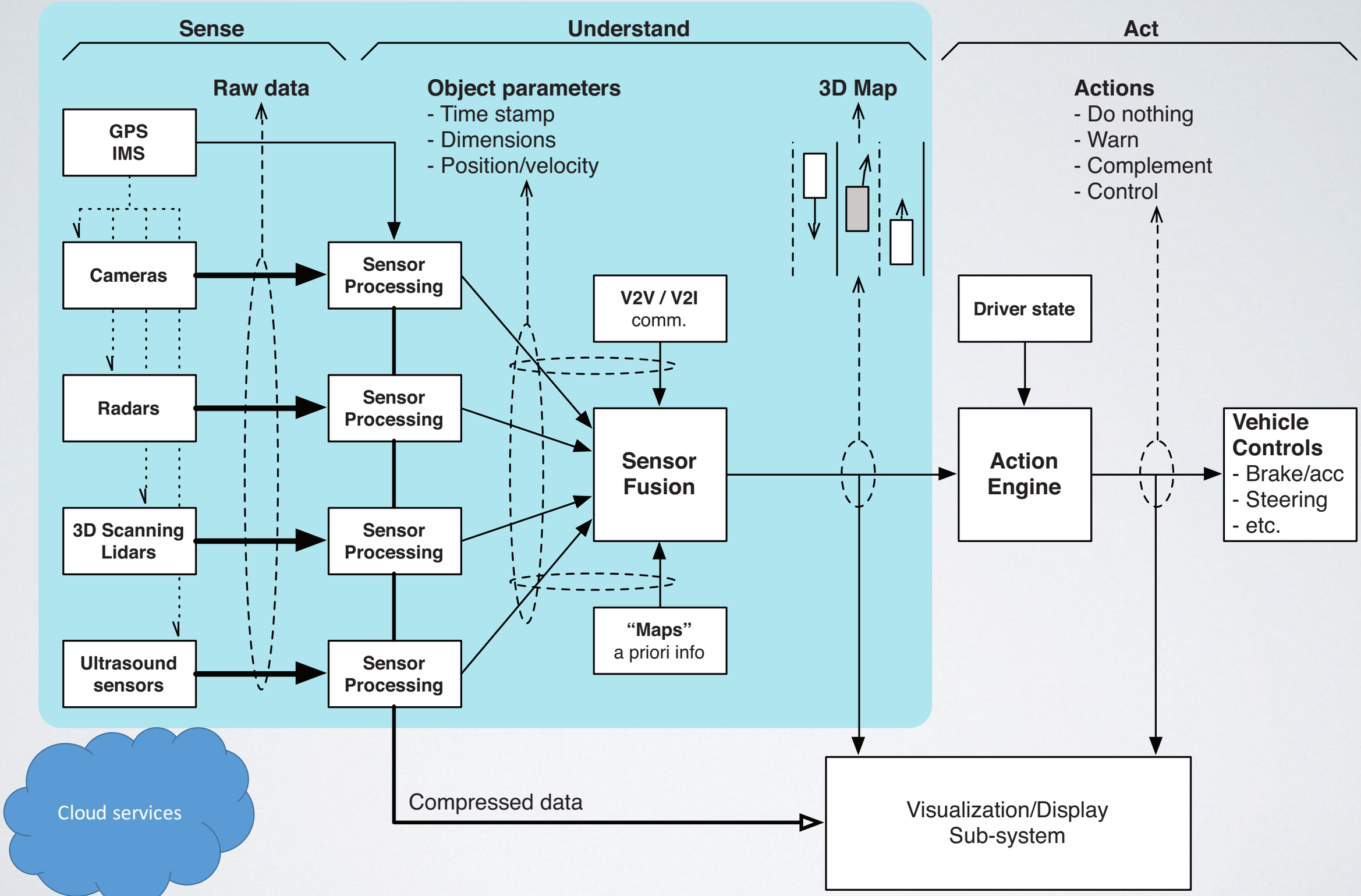
# CONSEQUENCE OF ATTACKS

- Level 2/3 automation: trigger handover to driver
- Level 4/5: trigger minimal risk condition (e.g. stop vehicle)
- Taking over control of vehicle (insurance fraud: can attackers steer cars of innocent people?)
- Install Advanced Persistent Threats, PII theft

| Sensor | Main attack | Main consequence | Main mitigation |
|---|---|---|---|
| LIDAR | Spoofing | Report fake object | Redundancy |
| RADAR | Spoofing | Report fake object | Redundancy |
| Ultrasonic sensor | Spoofing | Report fake object | Redundancy |
| Camera | Confusion | Detect wrong object | Robust neural network |
| Sensor fusion | Increase uncertainty | Wrong understandingof the situation | Bias estimation |
| GPS | Spoofing | Wrong driving decisions | Authenticated source, supersensitive quantum accelerometers |
| HD Maps | Poisoning | Wrong driving decisions | Non-repudiation, auditability |
| ECUs | escalated privileges | Unreliable (safety) system | Authentication, encryption |
| TCU (SOTA) | Wrong software update | system owned | Authentication, Integrity |

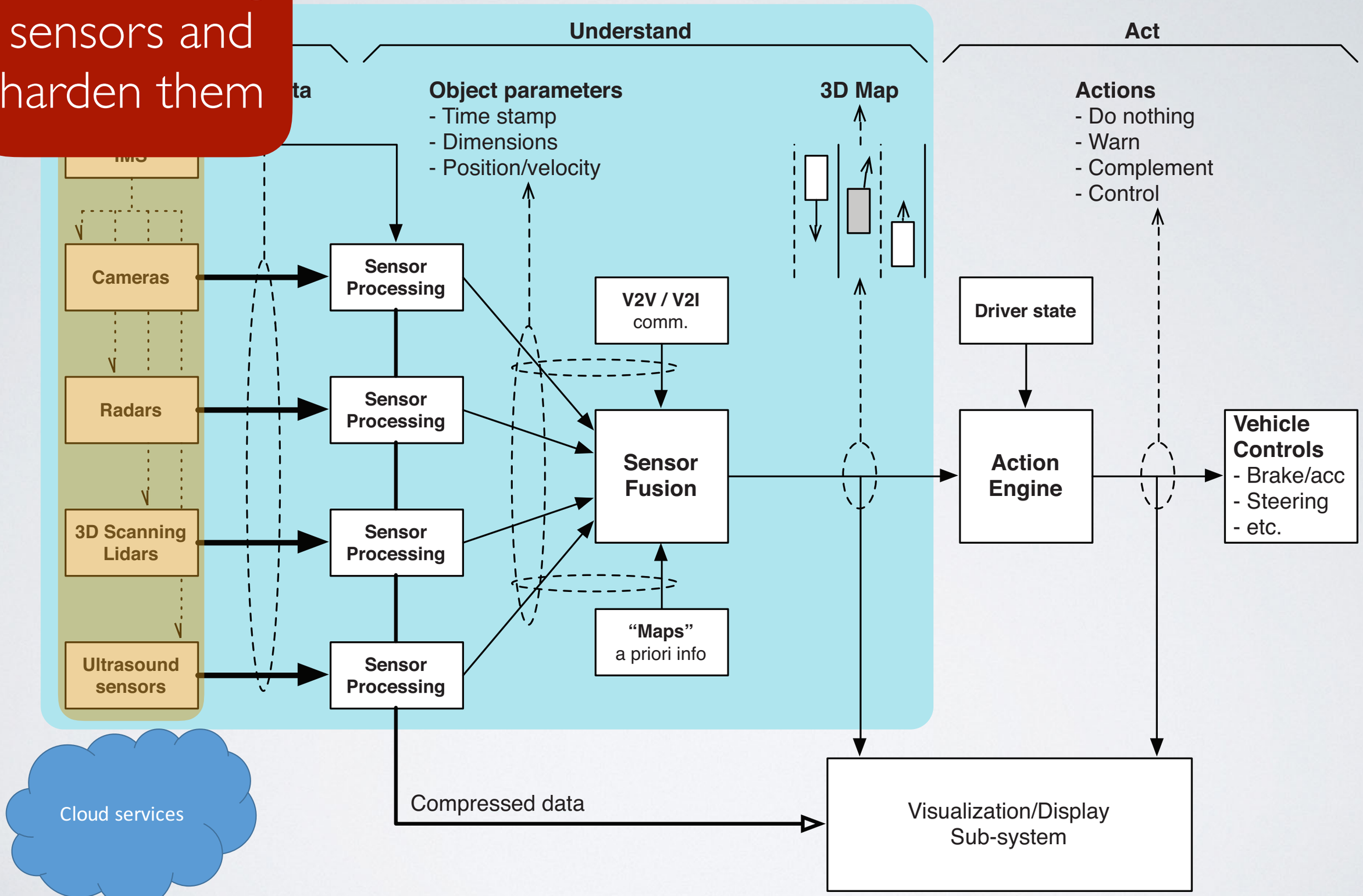
# COUNTERMEASURES

- **Prevention:**
  - Authentication (e.g. Physical Unclonable Function)
  - Encryption
  - Host-based security: virtualization, sandboxing
  - Sensor redundancy and sensor diversity
- **Detection:**
  - Misbehavior detection system (profile, prediction, context-aware)
  - Sensor redundancy and diversity
- **Reaction:**
  - Localization of attack
  - Recovery (in full, graceful degradation, safe shutdown)




credit: F. Mujica. Scalable electronics driving autonomous vehicle technologies. Technical report, Autonomous Vehicles R&D, Kilby Labs, Texas Instruments, 2014.

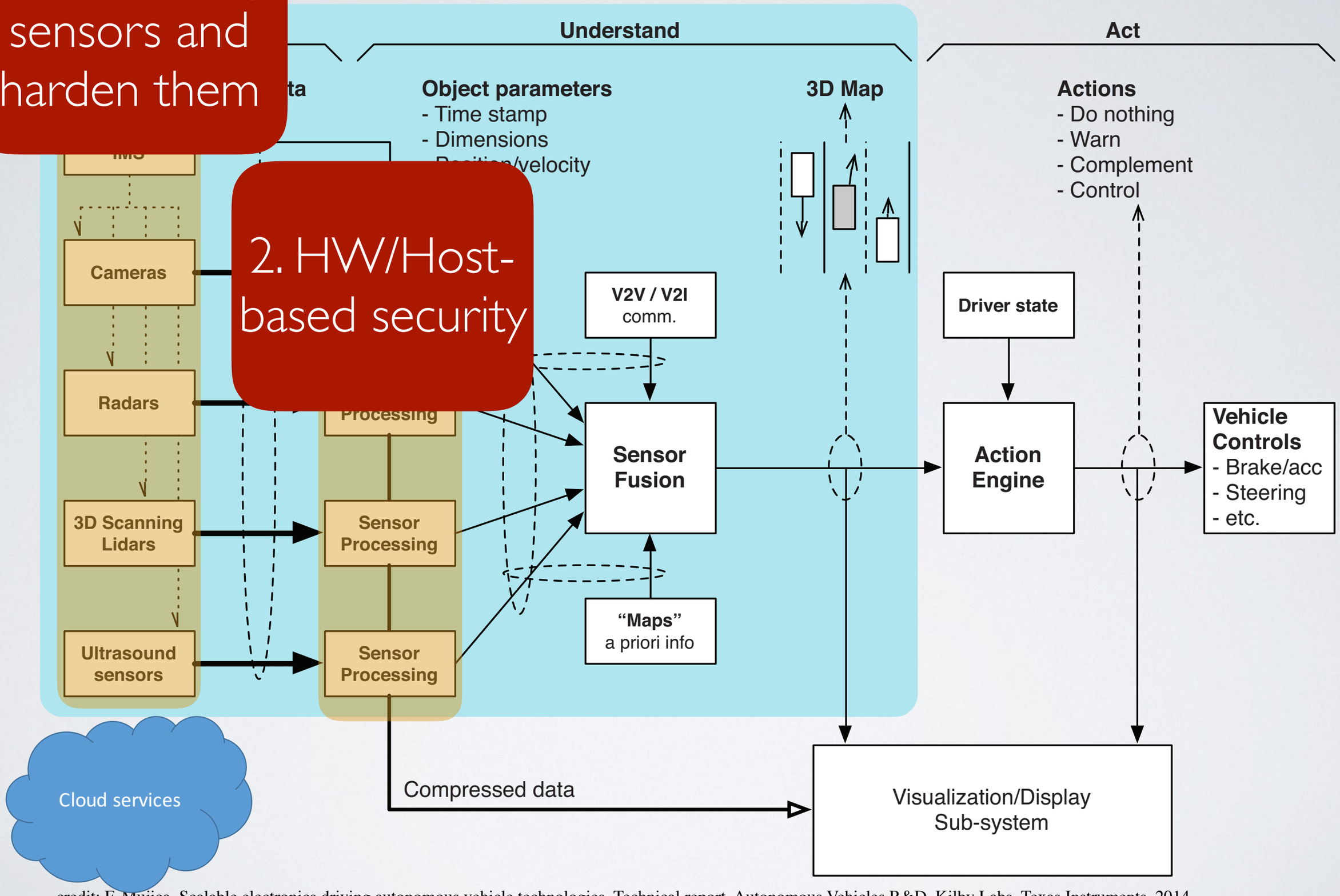
# 1. Pen-testing sensors and harden them




credit: F. Mujica. Scalable electronics driving autonomous vehicle technologies. Technical report, Autonomous Vehicles R&D, Kilby Labs, Texas Instruments, 2014.

1. Pen-testing sensors and harden them

2. HW/Host-based security

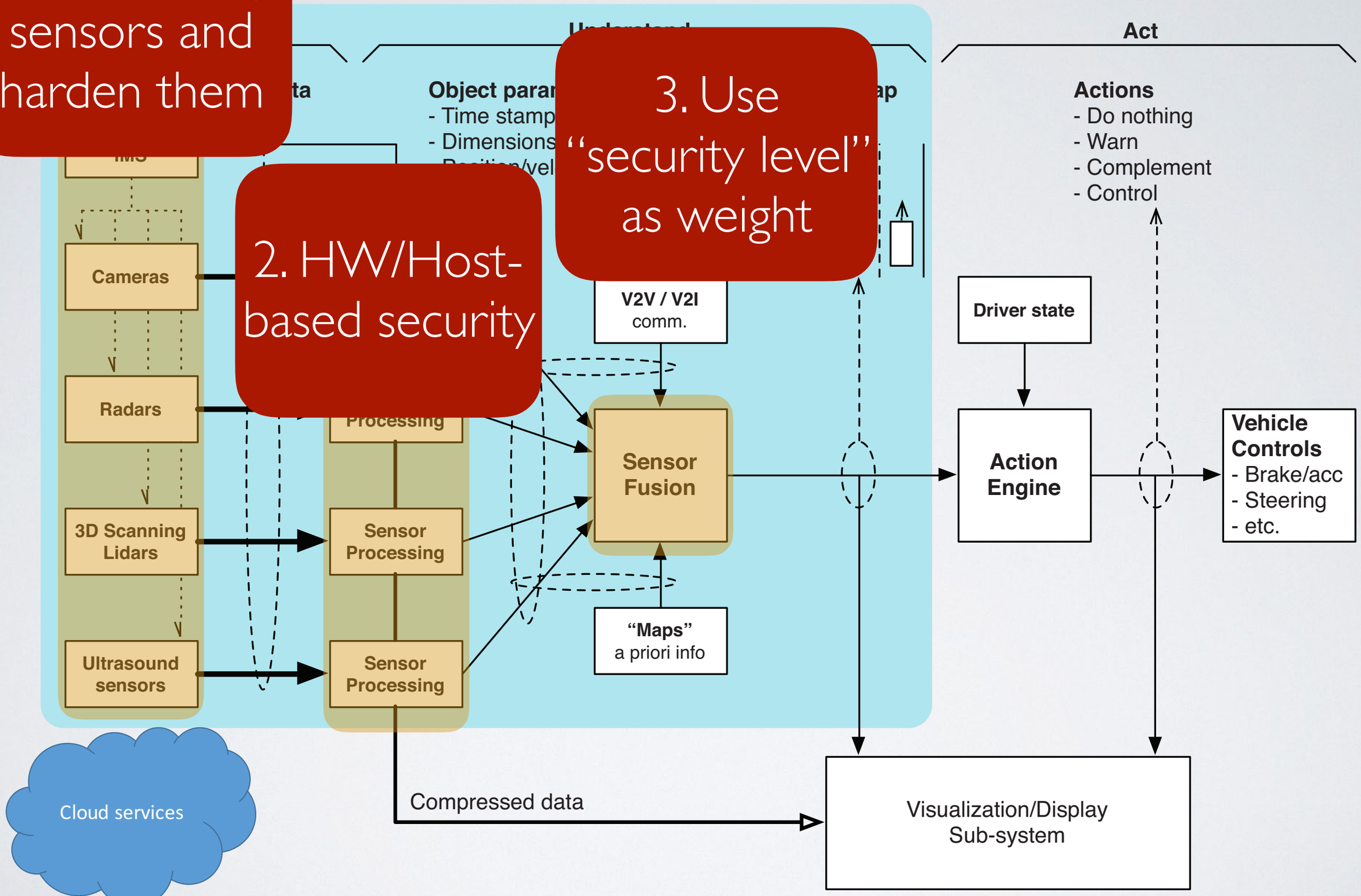



credit: F. Mujica. Scalable electronics driving autonomous vehicle technologies. Technical report, Autonomous Vehicles R&D, Kilby Labs, Texas Instruments, 2014.

1. Pen-testing sensors and harden them

2. HW/Host-based security

3. Use "security level" as weight



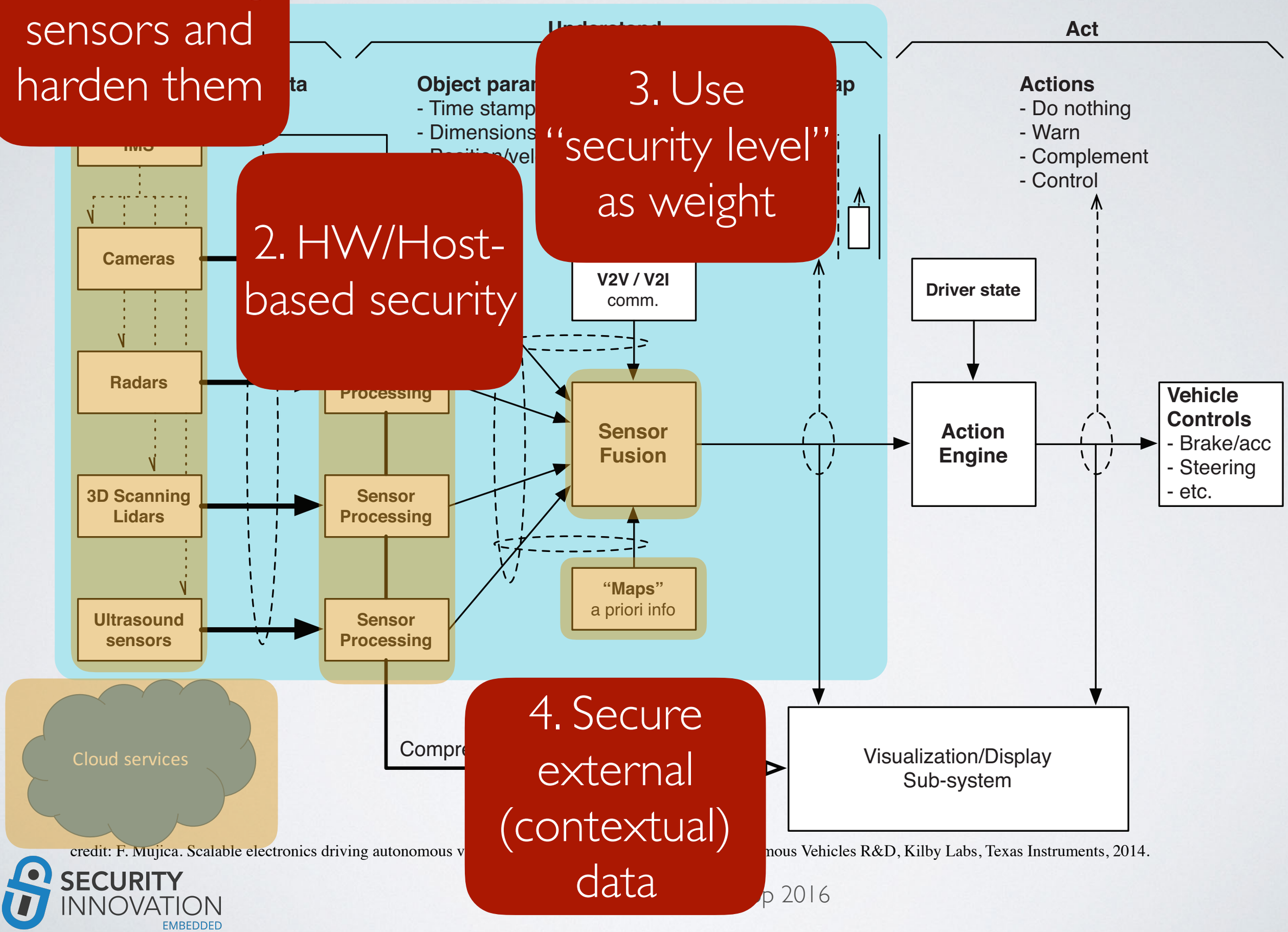

credit: F. Mujica. Scalable electronics driving autonomous vehicle technologies. Technical report, Autonomous Vehicles R&D, Kilby Labs, Texas Instruments, 2014.

1. Pen-testing sensors and harden them

2. HW/Host-based security

3. Use "security level" as weight

4. Secure external (contextual) data

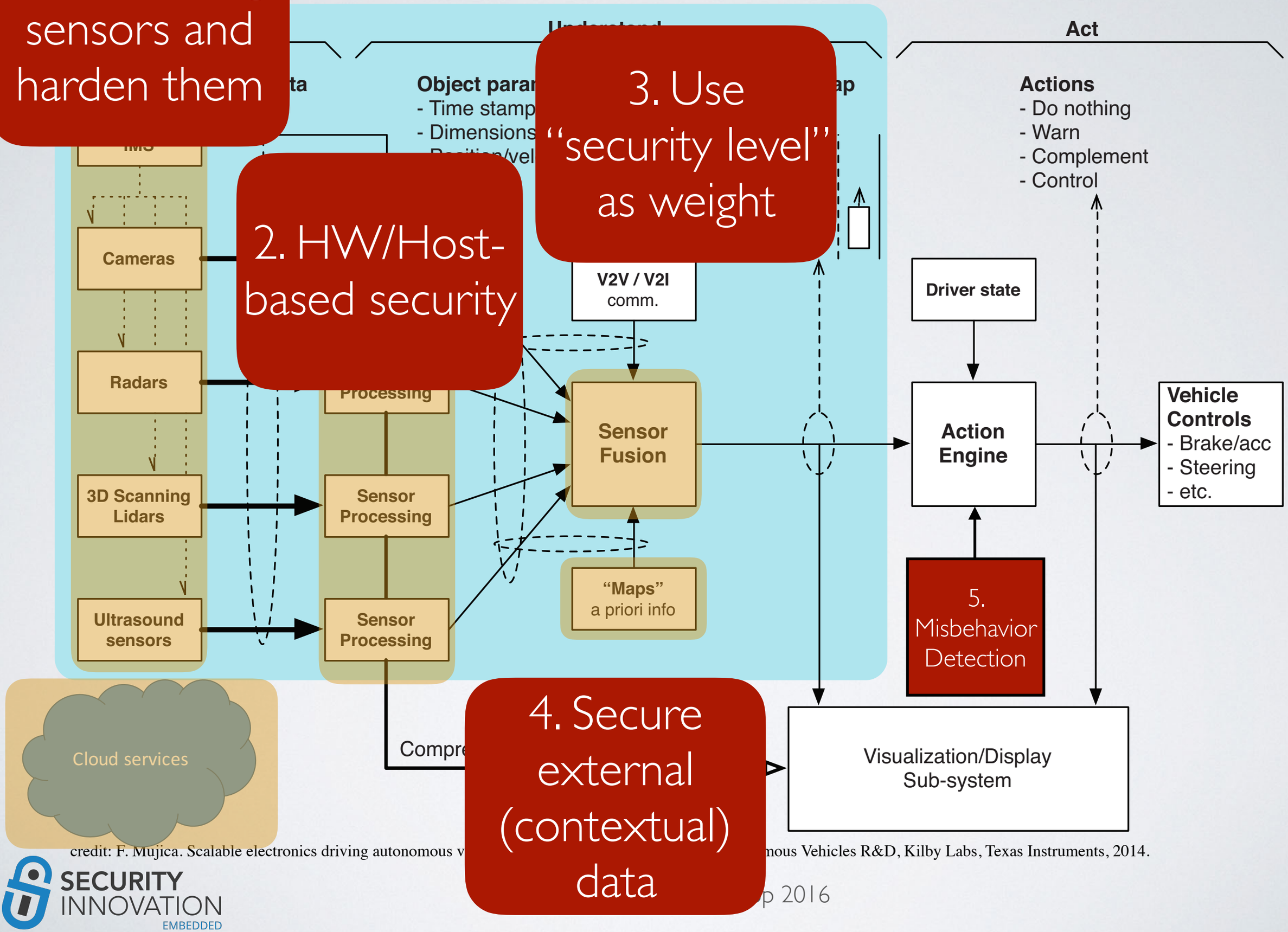



credit: F. Mujica. Scalable electronics driving autonomous v … mous Vehicles R&D, Kilby Labs, Texas Instruments, 2014.

1. Pen-testing sensors and harden them

2. HW/Host-based security

3. Use "security level" as weight




4. Secure external (contextual) data

credit: F. Mujica. Scalable electronics driving autonomous v … mous Vehicles R&D, Kilby Labs, Texas Instruments, 2014.

# Questions & Answers

Jonathan Petit
jpetit@securityinnovation.com